Extra help: FortiGuard

This section contains tips to help you with some common challenges of using FortiGuard.

FortiGuard services appear as expired/unreachable.

Verify that you have registered your FortiGate unit, purchased FortiGuard services and that the services have not expired at support.fortinet.com.

Services are active but still appear as expired/unreachable.

Verify that the FortiGate unit can communicate with the Internet by accessing FortiGate CLI and using the command `execute ping 8.8.8.8`. You can also use the `execute traceroute 8.8.8.8` command to troubleshoot connectivity to the Internet.

The FortiGate is connected to the Internet but can't communicate with FortiGuard.

If you have not done so already, verify your DNS settings and ensure that an unblocked port is being used for FortiGuard traffic.

If the FortiGate interface connected to the Internet gets its IP address using DHCP, go to **System > Network > Interfaces** and edit the Internet-facing interface. Ensure that **Override internal DNS** is selected.

Communication errors remain.

FortiGate units contact the FortiGuard Network by sending UDP packets with typical source ports of 1027 or 1031, and destination ports of 53 or 8888. The FDN reply packets would then have a destination port of 1027 or 1031. If your ISP blocks UDP packets in this port range, the FortiGate unit cannot receive the FDN reply packets.

In effort to avoid port blocking, You can configure your FortiGate unit to use higher-numbered ports, such as 2048-20000, using the following CLI command:

```
config system global
   set ip-src-port-range 2048-20000
end
```

Trial and error may be required to select the best source port range. You can also contact your ISP to determine the best range to use.